UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

TECSEC, INCORPORATED,
 	
           Plaintiff,
 	
      v.
 	
INTERNATIONAL BUSINESS MACHINES
CORPORATION, SAS INSTITUTE INC.,
SAP AMERICA, INC., SAP AG, CISCO
SYSTEMS, INC., SUN MICROSYSTEMS,
INC., SYBASE, INC., SOFTWARE AG,
SOFTWARE AG, INC., ADOBE SYSTEMS
INCORPORATED, EBAY INC., PAYPAL,
INC., and ORACLE CORPORATION,
 	
           Defendants.
	Case No. 1:10-cv-00115-LMB-TCB

**IBM'S BRIEF IN SUPPORT OF ITS PROPOSED CLAIM CONSTRUCTIONS
AND MOTION FOR SUMMARY JUDGMENT OF NO INFRINGEMENT**

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules

INTRODUCTION

TecSec brought this action on February 5, 2010, for alleged infringement of U.S. Patent Nos. 5,369,702; 5,680,452; 5,717,755; and 5,898,781 ("the '702 patent family"); 6,694,433 ("the '433 patent"); and 7,069,448 ("the '448 patent"), among others, inexplicably demanding that IBM pay over $530 million in damages—more than *175 times* the amount for which TecSec licensed its *entire patent portfolio* to Microsoft. This excessive demand is especially surprising given that the patents-in-suit bear little resemblance to the accused IBM products. Indeed, after extensive discovery demanded by TecSec—including expansive document requests requiring that IBM produce over 7 million pages of documents, over 40 depositions, and over 55 subpoenas on IBM's customers—TecSec's infringement case still rests on nothing but conjecture and a grab-bag of disparate documents and testimony that do not show what TecSec would like. Indeed, when the claims are construed in view of the intrinsic record as set forth in Exhibit 1—as they must be—there is no genuine dispute that IBM does not infringe.

TecSec nonetheless accuses a variety of IBM products and combinations of products of infringing 25 claims of the six patents-in-suit, including:

- '702 patent: claims 2, 8, 9, 12, 14, 15
- '781 patent: claims 1, 2, 3, 10, 13, 14, 15
- '755 patent: claims 1, 2
- '452 patent: claims 1, 2, 13
- '433 patent: claims 1, 3, 4, 8, 12
- '448 patent: claims 1, 5

The accused products fall into three general categories, including: (i) IBM DB2 and IDS database products (accused of infringing the '702 patent family); (ii) IBM WebSphere Application Server and DataPower Appliance products (accused of infringing the '702 patent family and '433 patent); and (iii) IBM System z mainframe server products (accused of infringing the '448 patent). But as discussed below, TecSec failed to come forth with sufficient evidence for several critical parts of its infringement case.   Summary judgment of no

1

infringement should therefore be granted on each issue set forth in Exhibit 2.[1] *See Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 249 (1986) ("[T]here is no issue for trial unless there is sufficient evidence favoring the nonmoving party for a jury to return a verdict for that party.").

STATEMENT OF UNDISPUTED MATERIAL FACTS

1.   The accused IBM database products do not provide multiple layers of encryption by nesting encrypted objects within other encrypted objects. (Rjaibi Decl. ¶¶ 6–8; Pickel Decl. ¶¶ 7–9; Leffler Decl. ¶¶ 7–8; Mandel Decl. ¶¶ 9–13; Jackson Decl. ¶¶ 6–9.)

2.   Under TecSec's allegedly infringing scenarios for the accused IBM database products, TecSec has no evidence that IBM ever performed every step, or made, used, sold, offered for sale, or imported the entire system of any claim of the '702 patent family.

3.   The accused IBM WebSphere products do not provide multiple layers of encryption by nesting encrypted objects within other encrypted objects. (Chung Decl. ¶¶ 8-9; Poon Decl. ¶¶ 9-10.)

4.   TecSec has no evidence that any single party both encrypted and decrypted the same object, or that any single party has implemented a system to both encrypt and access the same object, with the accused IBM WebSphere products, which cannot do so as sold by IBM.

5.   The accused IBM WebSphere products do not provide an object relating to a process that will undergo encryption, and TecSec has no evidence that either IBM or any other party ever provided a computer readable medium having stored thereon a first data set. (Chung Decl. ¶ 10; Poon Decl. ¶ 11.)

6.   The accused IBM WebSphere Application Server and DataPower XS40 and XI50 Appliances do not store encrypted information for use at a later time. (Chung Decl. ¶¶ 11-13; Poon Decl. ¶¶ 14-15.)

7.   The accused IBM System z products do not include a format filter adapted to extract control data and main data from input data. (Arnold Decl. ¶¶ 6–11.)

8.   TecSec has no evidence that the accused structure of any accused product is equivalent to any structure identified in the '702 patent specification that allegedly corresponds to any of the means-plus-function limitations of the '702 patent claims.

_____

[1] IBM specifically addresses only the applicable independent claims herein, because a finding of non-infringement of an independent claim requires a finding of non-infringement of all claims dependent thereon. *See Muniauction, Inc. v. Thomson Corp.*, 532 F.3d 1318, 1329 n.5 (Fed. Cir. 2008) ("A conclusion of noninfringement as to the independent claims requires a conclusion of noninfringement as to the dependent claims."). Accordingly, while not separately asserted, IBM also addresses independent claim 1 of the '702 patent (from which claim 2 depends) and independent claims 7 and 10 of the '433 patent (from which claims 8 and 12 depend).

9.   TecSec has no evidence of direct infringement of any of the asserted claims by any third party, that IBM had the specific intent to cause such infringement, or that IBM sold a non-staple component of a patented apparatus with knowledge that the component was especially made or adapted for use in an infringement.

LEGAL STANDARDS

I.   Summary Judgment.

Summary judgment should be entered where "the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). Where the defendant carries its burden of "pointing out to the district court that there is an absence of evidence to support the nonmoving party's case," the defendant is entitled to summary judgment. *Celotex Corp. v. Catrett*, 477 U.S. 317, 325 (1986). Thus, an accused infringer is entitled to summary judgment "where the patentee's proof is deficient in meeting an essential part of the legal standard for infringement." *Johnston v. IVAC Corp.*, 885 F.2d 1574, 1577 (Fed. Cir. 1989).

II.   Requirements For Proving Infringement.

"A patentee claiming infringement must present proof that the accused product meets each and every claim limitation." *Forest Labs., Inc. v. Abbott Labs.*, 239 F.3d 1305, 1310 (Fed. Cir. 2001). The patentee must also prove that the accused infringer either directly infringed the patent under 35 U.S.C. § 271(a) or indirectly infringed the patent under 35 U.S.C. § 271(b) or (c). Failure to do so warrants summary judgment of no infringement. *Celotex*, 477 U.S. at 325.

A.   Direct Infringement.

To establish direct infringement, the patentee must establish that the alleged infringer either made, used, offered to sell, or sold in the United States, or imported into the United States, the patented invention. *See* 35 U.S.C. § 271(a). But while "[d]irect infringement is a strict-liability offense, … it is limited to those who practice ***each and every*** element of the claimed

3

invention." *BMC Res., Inc. v. Paymentech, L.P.*, 498 F.3d 1373, 1381 (Fed. Cir. 2007).[2] The

Federal Circuit has thus made clear that "liability for infringement requires a party to make, use,

sell, or offer to sell the patented invention, ***meaning the entire patented invention***." *Id*. at 1380.

Accordingly, a person who makes, uses, sells, offers to sell, or imports less than the ***entire***

patented invention is not a direct infringer as a matter of law. *See Rotec Indus., Inc. v.

Mitsubishi Corp.*, 215 F.3d 1246, 1252 n.2 (Fed. Cir. 2000) ("[O]ne may not be held liable under

§ 271(a) for 'making' or 'selling' less than a complete invention.").

B.   Indirect Infringement.

"When a defendant participates in or encourages infringement but does not directly

infringe a patent, the normal recourse under the law is for the court to apply the standards for

liability under indirect infringement." *BMC Res.*, 498 F.3d at 1378. Indirect infringement may

include "inducing infringement" or "contributory infringement." 35 U.S.C. §§ 271(b) and (c).

Inducing Infringement: To establish inducing infringement, a patentee must establish

that the alleged infringer "actively induces infringement of a patent." 35 U.S.C. § 271(b).

However, as a required predicate, the patentee must establish that some other party committed

the entire act of direct infringement. *See BMC Res.*, 498 F.3d at 1380; *Novartis Pharms. Corp. v.

Eon Labs Mfg., Inc.*, 363 F.3d 1306, 1308 (Fed. Cir. 2004). Additionally, the patentee must

establish that the alleged infringer knowingly induced the infringement and possessed specific

intent to encourage the infringement. *See ACCO Brands, Inc. v. ABA Locks Mfr. Co.*, 501 F.3d

1307, 1312 (Fed. Cir. 2007). Accordingly, "[t]he plaintiff has the burden of showing that the

alleged infringer's actions induced infringing acts and that he knew or should have known his

---

[2] All emphasis added unless otherwise noted.

actions would induce actual infringements." *DSU Med. Corp. v. JMS Co.*, 471 F.3d 1293, 1304 (Fed. Cir. 2006) (*en banc* in relevant part) (citation omitted). Mere knowledge by the alleged infringer is not enough—specific intent and actions to induce infringement must be proven. *Warner-Lambert Co. v. Apotex Corp.*, 316 F.3d 1348, 1364 (Fed. Cir. 2003).

  Contributory Infringement: To establish contributory infringement, a patentee must establish that the alleged infringer offered to sell or sold a component of a patented apparatus that constitutes a material part of the invention, with knowledge that the component is especially made or adapted for use in an infringement, and not a staple article suitable for substantial noninfringing use. *See* 35 U.S.C. § 271(c). As with inducing infringement, contributory infringement requires, as a predicate, that some other party committed the entire act of direct infringement. *See BMC Res.*, 498 F.3d at 1379. Similarly, the alleged infringer's state of mind is an essential element of contributory infringement. *See id*. at 1381 ("Another form of indirect infringement, contributory infringement under § 271(c), also requires a *mens rea* (knowledge) and is limited to sales of components or materials without substantial noninfringing uses.").

<div align="center">**ARGUMENT**</div>

I. **IBM's Database Products Do Not Infringe The '702 Patent Family.[3]**

  TecSec accuses several alleged implementations of IBM's DB2 and IDS database products of infringing the asserted claims of the '702 patent family in six "scenarios," as follows:

    Scenario 1: DB2 for z/OS (versions 8+) used in combination with the IBM Data Encryption for IMS and DB2 Databases tool ("Data Encryption Tool"), where the claimed "object" is a table in a DB2 database;

---

[3] Descriptions of the accused IBM database products are provided in the declarations of James Pickel (DB2 for z/OS), Walid Rjaibi (DB2 for LUW), Jonathan Leffler (IDS), Geoff Jackson (Data Encryption Tool), and Peter Mandel (DEE), filed concurrently herewith.

Scenario 2: DB2 for z/OS (versions 8+) using the built-in "column-level encryption," where the claimed "object" is a column within a table in a DB2 database;

Scenario 3: DB2 for LUW (versions 9.1+) using the built-in "column-level encryption," where the claimed "object" is a column within a table in a DB2 database;

Scenario 4: DB2 for LUW (versions 8.2+ with Fixpack 14) using the IBM Database Encryption Expert ("DEE"), where the claimed object is non-metadata file contents of the DB2 database tablespace;

Scenario 5: IDS (versions 10+) using the built-in "column-level encryption" applied to the data within a column in a table in an IDS database; and

Scenario 6: IDS (versions 11+) with an instance of DEE (at least version 1.1 with Fix Pack 3 for IDS version 11.X support) for encryption of the non-meta data portions of a tablespace of an IDS database.

As set forth below, TecSec's infringement claims fail as a matter of law because: (i) none of the accused "scenarios" provide "multi-level security"; and (ii) IBM does not directly infringe because IBM has not performed *every* step of the asserted method claims nor made, used, sold, offered for sale, or imported the *entire* claimed system.

A.   The Accused Database Products Do Not Provide "Multi-Level Security."

1.   Claim Construction.

#	Claim Term	Proposed Construction
1	"multi-level security"	"encrypted objects are nested within other objects which are also encrypted, possibly within other objects, resulting in multiple layers of encryption"
2	"multimedia"	"a computer technology that displays information using a combination of full-motion video, animation, sound, graphics and text with a high degree of user interaction"

a.   The Preamble Is A Claim Limitation.

The phrase "multi-level multimedia security" appears in the preamble of every independent claim of the '702 patent family. (Exs. 3–6.)   Here, the preamble is a claim limitation that cannot be ignored. "In considering whether a preamble limits a claim, the preamble is analyzed to ascertain whether it states a necessary and defining aspect of the invention, or is simply an introduction to the general field of the claim." *On Demand Mach.*

6

Corp. v. Ingram Indus., Inc., 442 F.3d 1331, 1343 (Fed. Cir. 2006).   "The effect preamble language should be given can be resolved only on review of the entirety of the patent to gain an understanding of what the inventors actually invented and intended to encompass by the claim." *Corning Glass Works v. Sumitomo Elec. U.S.A., Inc.*, 868 F.2d 1251, 1257 (Fed. Cir. 1989).

"Multi-level multimedia security" is clearly a defining aspect of the invention and thus a limitation. For example, the '702 patent highlights the critical "multi-level multimedia security" throughout the specification—the Abstract (Ex. 3), all the figures (*id.*), the Field of the Invention (*id.* at 1:8–11), the Background of the Invention (*id.* at 3:7–9), the Summary of the Invention (*id.* at 4:22–34), the Detailed Description of the Invention (*id.* at 5:8–41, 6:36–39, 7:50–57, 11:18–35), and every independent claim (*id.* at 12:2–14:30).   The preamble cannot, therefore, be disregarded as a claim limitation. *See Poly-Am., L.P. v. GSE Lining Tech., Inc.*, 383 F.3d 1303, 1310 (Fed. Cir. 2004) (finding the preamble phrase "blown-film" is a limitation because "[t]he specification is replete with references to the invention as a 'blown-film' liner, including the title of the patent itself and the 'Summary of the Invention,'" demonstrating that "the inventor considered that the 'blown-film' preamble language represented an important characteristic of the claimed invention."); *Gen. Elec. Co. v. Nintendo Co.*, 179 F.3d 1350, 1361–62 (Fed. Cir. 1999) (finding the preamble phrase "bit map display device" is a limitation because "[i]n light of the specification, to read the claim indiscriminately to cover all types of display systems would be divorced from reality.").

Further evidencing that the preamble is a limitation, the patentee expressly relied upon it to distinguish the prior art Preston patent during prosecution.   For example, the patentee distinguished the Preston patent because it allegedly could not "cryptographically embed devices within other devices or within data files," *i.e.*, could not provide "multi-level security":

7

> In contrast, Preston et al. ("Preston") discloses a multiple user stored data cryptographic labeling system that uses labels to control access to data files. Objects other than data files are not controlled by the Preston system, and even these data file objects are not disclosed as having the capability of being cryptographically embedded according to the Preston system. The Preston system can enable a user to lock a particular data file to a particular computer, but cannot cryptographically embed devices within other devices or within data files.

(Ex. 7 at IBMTS002635674.) The preamble must therefore be construed as a claim limitation. *See Catalina Mktg. Int'l, Inc. v. Coolsavings.com, Inc.*, 289 F.3d 801, 808 (Fed. Cir. 2002) ("[C]lear reliance on the preamble during prosecution to distinguish the claimed invention from the prior art transforms the preamble into a claim limitation.").

Finally, TecSec repeatedly relied upon "multi-level multimedia security" to rebut IBM's invalidity contentions, further demonstrating that it must be construed as a limitation for purposes of infringement. *See Amgen Inc. v. Hoechst Marion Roussel, Inc.*, 314 F.3d 1313, 1330 (Fed. Cir. 2003) ("It is axiomatic that claims are construed the same way for both invalidity and infringement."). For example, TecSec relied upon the preamble in response to IBM's Interrogatory No. 15 to distinguish the prior art. (Ex. 8 at 4.) TecSec's expert also relied upon the preamble to distinguish the prior art. (Ex. 9 at 35 ("Many '702 patent family claims recite 'multilevel … security.' The '707 patent fails to disclose this feature."), 47 ("Preston fails to disclose 'multimedia security' as recited by at [sic] the claims."); *see also id*. at 53, 55, 57, 58, 61.) Indeed, TecSec argued in its opening summary judgment brief that the multi-level security concept is *essential* to the '702 patent family. (D.I. 417 at 8 ("This embedding of encrypted objects within other objects creates the 'multi-level security' that is *essential* to the DCOM Patents."). The preamble is therefore a claim limitation. *See Computer Docking Station Corp. v. Dell, Inc.*, 519 F.3d 1366, 1375 (Fed. Cir. 2008) ("The written description and applicants'

8

statements during prosecution emphasize this feature of the invention, yet this limitation does not appear in the body of the claims. As a result, this court finds that the terms … limit the scope of the asserted claims."); *Jansen v. Rexall Sundown, Inc.*, 342 F.3d 1329, 1333 (Fed. Cir. 2003).

> **b.** **The Patentee Defined "Multi-Level Multimedia Security" During Prosecution To Overcome The Examiner's Rejection.**

During prosecution, the examiner rejected claim 1—the only claim pending at the time—as indefinite under 35 U.S.C. § 112, second paragraph, because the examiner concluded that "it is unclear what is meant by 'multi-level multimedia security'" in the context of the patent:

> Claim 1 is rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
>
> On line 1 of independent claim 1, it is unclear what is meant by "multi-level multimedia security".

(Ex. 7 at IBMTS002635653.) To overcome this rejection, the patentee amended the patent "to more clearly explain" the term:

> The specification has been amended to more clearly explain the terms "object" and "Multi-level multimedia security". Multi-level multimedia security is further described on page 8, from lines 1-8. These terms are well known to those of ordinary skill in the art. See Dyson, Peter *The PC User's Essential Accessible Pocket Dictionary*. No new matter has been added by this amendment.

(*Id*. at IBMTS002635672.) Specifically, the patentee amended the patent to clarify that "[m]ulti-level security is achieved because *encrypted objects may be nested within other objects which are also encrypted*, possibly within other objects, resulting in *multiple layers of encryption*":

> Page 6, line 20, after "achieved," insert ⁀ Multi-level security is achieved because encrypted objects may be nested within other objects which are also encrypted, possibly within other objects, resulting in multiple layers of encryption. Multimedia security is achieved because objects are encrypted. Where other encryption systems encrypt only files or other data, the system of the present invention encrypts any object, encompassing all forms of media. Thus, the nesting of individually encrypted objects provides security that is multi-level and multimedia. ⁀

(*Id.* at IBMTS002635664; *see also* Ex. 3 at 4:25–28.)

In addition to expressly defining "multi-level security," the applicant also defined "multimedia" by amending the patent and providing a dictionary definition. Specifically, the patentee amended the patent to explain that because the patented system secures multimedia, the "invention encrypts *any* object, encompassing *all* forms of media." (Ex. 7 at IBMTS002635664.) Then, the applicant directed the examiner to the *Dyson* dictionary:

> The specification has been amended to more clearly explain the terms "object" and "Multi-level multimedia security". Multi-level multimedia security is further described on page 8, from lines 1-8. These terms are well known to those of ordinary skill in the art. See Dyson, Peter *The PC User's Essential Accessible Pocket Dictionary*. No new matter has been added by this amendment.

(*Id.* at IBMTS002635672.) This dictionary expressly defines "multimedia"[4] as "a computer technology that displays information using a combination of full-motion video, animation, sound, graphics and text with a high degree of user interaction":

> **multimedia** A computer technology that displays information using a combination of *full-motion video*, *animation*, sound, graphics and text with a high degree of user interaction.
> See also *hypermedia*, *hypertext*.

(Ex. 10 at 354.) In view of this definition and explanation, the examiner withdrew his indefiniteness rejection. (Ex. 7 at IBMTS002635680.)

The patentee's unambiguous reliance upon the dictionary definition of "multimedia" and clarification of the meaning of the term "multi-level security" during prosecution to overcome the examiner's indefiniteness rejection is therefore binding as a matter of law. *See Honeywell Inc. v. Victor Co. of Japan, Ltd.*, 298 F.3d 1317, 1323–24, 1328 (Fed. Cir. 2002) (reversing

---

[4] In contrast, the term "multi-level" does not appear in the cited dictionary.

district court's construction of the term "contiguous" because the court improperly modified the inventor's definition taken from a standard English dictionary during prosecution.). Indeed, the Federal Circuit has held that when a patentee relies upon a particular meaning of a term during prosecution, as the patentee did here, this meaning is "***binding in litigation***":

> *[T]hrough statements made during prosecution* or reexamination an applicant for a patent or a patent owner, as the case may be, *may commit to a particular meaning for a patent term, which meaning is then binding in litigation*.

CVI/Beta Ventures, Inc. v. Tura LP, 112 F.3d 1146, 1158 (Fed. Cir. 1997); *see also Medrad, Inc. v. MRI Devices Corp.*, 401 F.3d 1313, 1318 (Fed. Cir. 2005) ("A patentee may define a particular term in a particular way, and in that event the term will be defined in that fashion for purposes of that particular patent, no matter what its meaning in other contexts.") (citation omitted); *Home Diagnostics, Inc. v. LifeScan, Inc.*, 381 F.3d 1352, 1356 (Fed. Cir. 2004) ("As in the case of the specification, a patent applicant may define a term in prosecuting a patent."). Accordingly, the Court should construe these terms as set forth above.

c.   The Patentee's Definition Is Consistent With The Patent Specification.

Consistent with the patentee's definition of "multi-level multimedia security" adopted during prosecution, the specification repeatedly and consistently characterizes the invention as nesting or embedding encrypted objects within other encrypted objects, resulting in multiple layers of encryption. For example, in the "Summary of the Invention" section, the patent explains that one of the objectives of the invention is to embed objects within other objects "resulting in an access hierarchy for users of the system." (Ex. 3 at 3:21–24.) The patent further explains that once encrypted objects are embedded in a standard container object, the container object is also encrypted, *i.e.*, encrypted objects are embedded within another encrypted object:

11

> The DCOM has a standard Multi-Level Security object interface **2** that interfaces with the plain text container object's encrypted embedded object(s) **4**. It does this through a standard application **6** that has the capability to embed an object in a container object, such as Microsoft's Object Package for Windows. After the Encrypted object(s) is/are embedded in a standard container object(s) **10** and the container object(s) **10** is/are encrypted, the original encrypted object(s) and the new encrypted container object(s) is/are ready for transport.

(*Id.* at 5:32–41.)

All the examples of the invention identified in the patent specification implement this same multiple-layer encryption concept. For example, the patent explains that the invention manages and tracks one or more embedded encrypted objects within other encrypted objects:

> The first example shows the ability for OOKeyMan to securely manage and track single or multiple embedded encrypted objects within other encrypted objects. This is done with a single application.
> The second example shows the ability for OOKeyMan to securely manage and track single or multiple embedded encrypted objects within other encrypted objects. The embedded encrypted objects can even be part of encrypted objects from other applications.

(*Id.* at 7:50–58.) And Figure 3 shows an encrypted object with a web of embedded encrypted objects nested within other encrypted objects, resulting in multiple layers of encryption:

> FIG. 3 and FIG. 4 show an encrypted object that contains a web of embedded encrypted objects nested within the other encrypted objects. The object shown in FIG. 3 contains ten embedded encrypted objects at five various levels. The encrypted object embedded in level 5 was embedded in an object in level four, level four objects in level 3 and so on. The plain text object containing the level 5 encrypted object can then be encrypted for further security. This single encrypted object encapsulates all of the data associated with the encrypted objects within it and therefore the entire encrypted object can then be sent out via any transport mechanism supporting binary file transfer.
> FIG. 4 shows an encrypted object that contains a web of embedded encrypted objects nested within it. All of the attached embedded encrypted objects are fused together resulting in a single encapsulated encrypted object. The DCOM is powerful enough to dynamically adapt to accommodate N dimensional objects.
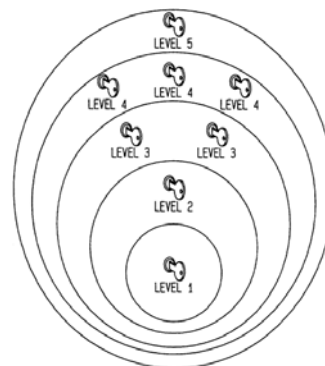
FIG. 3

(*Id.* at 11:18–36, Fig. 3; *see also id.* at 4:47–49, 4:52–54, Figs. 4, 6, 8.)

Accordingly, consistent with the patentee's definition provided during prosecution to overcome the examiner's indefiniteness rejection, and consistent with the patentee's description of the invention in the specification, the Court should construe these terms as set forth above.

12

Phillips v. AWH Corp., 415 F.3d 1303, 1316 (Fed. Cir. 2005) ("Ultimately, the interpretation to be given a term can only be determined and confirmed with a full understanding of what the inventors actually invented and intended to envelop with the claim.") (citation omitted).

2.   There Is No Dispute That The Accused Database Products Do Not Provide "Multi-Level Security"

Every independent claim of the '702 patent family requires a system or method for providing "multi-level security" in a data network, *i.e.*, that "encrypted objects are nested within other objects which are also encrypted, possibly within other objects, resulting in multiple layers of encryption." (Ex. 3–6.) But there is no genuine dispute that *none* of the accused scenarios do so—each provides, at most, only a single layer of encryption. Indeed, TecSec identified no evidence that any accused scenario is capable of providing multiple layers of encryption.[5] In fact, TecSec identified only *one* allegedly encrypted "object" for each scenario ("a table," "a column within a table," "non-metadata file contents," or "non-metadata portions of a tablespace"). TecSec cannot, therefore, demonstrate that the accused scenarios provide "encrypted objects [that] are nested within other objects which are also encrypted." Moreover, TecSec provided no explanation for how each accused scenario allegedly achieves "multi-level security," but rather, made only conclusory assertions and cited various documents—without explanation—that provide no support for this limitation.[6] (Clark Decl. ¶ 25.)

---

[5] TecSec provided no evidence of infringement under the doctrine of equivalents for this term, so TecSec's claims are limited to literal infringement. *See Schoell v. Regal Marine Indus., Inc.*, 247 F.3d 1202, 1210 (Fed. Cir. 2001).

[6] TecSec misleadingly cites documents using the phrase "multi-level security." But this capability is entirely unrelated to encryption. Rather, it refers to mechanisms for protecting information by identifying users and privileges based on the DOD "Orange Book" published in 1983—nearly a decade before TecSec filed its patents on encryption security. (Clark Decl. ¶ 25.)

TecSec's lack of evidence is not surprising given that each of the six accused scenarios is *incapable* of performing encryption at more than one level, and cannot nest encrypted objects within other encrypted objects. (Rjaibi Decl. ¶¶ 6–8; Pickel Decl. ¶¶ 7–9; Leffler Decl. ¶¶ 7–8; Mandel Decl. ¶¶ 9–13; Jackson Decl. ¶¶ 6–9.) For example, in accused scenario 1, the IBM Data Encryption Tool *can only encrypt an entire table*—it is incapable of nesting encrypted objects within other encrypted objects or providing multiple layers of encryption. (Jackson Decl. ¶¶ 6– 9.) Similarly, in accused scenarios 2, 3, and 5, the built-in "column-level encryption" functionality of DB2 and/or IDS cannot nest encrypted objects within other encrypted objects or provide multiple layers of encryption. (Rjaibi Decl. ¶¶ 6–8; Pickel Decl. ¶¶ 7–9; Leffler Decl. ¶¶ 7–8.) And in accused scenarios 4 and 6, the IBM Database Encryption Expert ("DEE") is *only capable of encryption at the file-level*—it cannot nest encrypted objects within other encrypted objects or provide multiple layers of encryption. (Mandel Decl. ¶¶ 9–13.)

Moreover, despite the Court's explicit Order that TecSec identify exactly where in IBM's source code each and every claim element is allegedly found in response to IBM's Interrogatory No. 17 (D.I. 364), TecSec provided *no* source code citation for the "multi-level security" element. (Ex. 16 at Ex. 1 at 3.) And with good reason. No such source code exists, because the accused products simply do not provide the claimed "multi-level security." (Rjaibi Decl. ¶¶ 6–8; Pickel Decl. ¶¶ 7–9; Leffler Decl. ¶¶ 7–8; Mandel Decl. ¶¶ 9–13; Jackson Decl. ¶¶ 6–9.) This failure to identify any evidence of "multi-level security" is fatal to TecSec's infringement claims, so summary judgment of no infringement should be granted. *See Exigent Tech., Inc. v. Atrana Solutions, Inc.*, 442 F.3d 1301, 1309 (Fed. Cir. 2006) ("[N]othing more is required than the filing of a summary judgment motion stating that the patentee had no evidence of infringement and pointing to the specific ways in which accused systems did not meet the claim limitations.").

> **B.   IBM Does Not Directly Infringe By Making, Using, Selling, Offering For Sale, Or Importing The Accused Database Products.**

TecSec accuses IBM of *directly* infringing each asserted claim of the '702 patent family, including both the method claims and system claims. But there is no evidence that IBM ever performed every claimed step or made, used, sold, or offered to sell the entire claimed system.

Method Claims: To show that IBM directly infringed the method claims, TecSec must show that *IBM* performed *every* step of the claimed method. *See Joy Techs., Inc. v. Flakt, Inc.*, 6 F.3d 770, 775 (Fed. Cir. 1993) ("A method claim is directly infringed only by one practicing the patented method."); *BMC Res.*, 498 F.3d at 1381 ("Direct infringement is a strict-liability offense … limited to those who practice each and every element of the claimed invention."). But TecSec failed to come forth with any evidence that IBM performed *any* of the steps of the method claims. Instead, TecSec contends that IBM's customers may have performed the claimed steps. But even if true, this does not constitute direct infringement by IBM as a matter of law. *Id.*

System Claims: To show that IBM directly infringed the system claims, TecSec must show that *IBM* made, used, sold, offered for sale, or imported the *entire* claimed system. *See Rotec*, 215 F.3d at 1252 n.2 ("[O]ne may not be held liable under § 271(a) for 'making' or 'selling' less than a complete invention."); *BMC Res.*, 498 F.3d at 1380 ("[L]iability for infringement requires a party to make, use, sell, or offer to sell the patented invention, *meaning the entire patented invention*."). Again, TecSec failed to come forth with any evidence that IBM has done so. Instead, TecSec simply accuses IBM software—at most only a *part* of the claimed system—which *users* may install on a computer system and allegedly configure into one of the six accused scenarios. (Ex. 17 at 15 ("At a *user's* direction, any one of four different access control techniques is implemented by DB2, z/OS or the Tool.").) Even if some user-implemented system met all the asserted claim limitations—which it does not—IBM cannot be

held liable for direct infringement as a matter of law, because it is undisputed that **IBM** did not

make, use, sell, offer to sell, or import the *entire* accused system. *See BMC Res.*, 498 F.3d at

1380. TecSec's direct infringement claims thus fail as a matter of law, and summary judgment

of no direct infringement should be granted. *See Anderson*, 477 U.S. at 249.

II.   IBM's WebSphere Products Do Not Infringe The '702 Patent Family.[7]

TecSec accuses the following IBM WebSphere products of infringing the asserted claims

of the '702 patent family (the '702, '781, '755, and '452 patents):

- Websphere Application Server (versions 6.1+);
- WebSphere DataPower XML Security Gateway XS40 (versions 2.5+);
- WebSphere DataPower Integration Appliance XI50 (versions 3.1+); and
- WebSphere DataPower B2B Appliance XB60 (versions 3.7+).

As set forth below, TecSec's infringement claims fail as a matter of law because: (i) none of the

accused WebSphere products provide "multi-level security" as required by every asserted claim;

and (ii) no single party performs the entire act of alleged infringement.

A.   The Accused WebSphere Products Do Not Provide "Multi-Level Security."

As discussed above, every independent claim of the '702 patent family requires a system

or method for providing "multi-level security" in a data network, *i.e.*, providing that "encrypted

objects are nested within other objects which are also encrypted, possibly within other objects,

resulting in multiple layers of encryption." As sold by IBM, however, none of the accused

WebSphere products provide multiple layers of encryption. (Chung Decl. ¶¶ 8-9; Poon Decl. ¶¶

9-10.) And TecSec identified no evidence that they do. Indeed, although the Court expressly

---

[7] Descriptions of the accused IBM WebSphere products are provided in the declarations of Hyen Chung (WebSphere Application Server) and Shiu-Fun Poon (WebSphere DataPower products), filed concurrently herewith.

ordered TecSec to identify exactly where in IBM's source code every claim element is allegedly found (D.I. 364), TecSec provided *no* source code citation for the "multi-level security" element. (Ex. 16 at Ex. 9 at 1.) This failure stems from the fact that no such source code exists—the WebSphere products as sold simply do not perform the claimed "multi-level security." (Chung Decl. ¶¶ 8-9; Poon Decl. ¶¶ 9-10.) TecSec's failure to identify evidence of "multi-level security" is fatal to TecSec's infringement claims, and summary judgment of no infringement should therefore be granted.[8] *See Exigent*, 442 F.3d at 1309.

B.   No Single Party Performs The Entire Act Of Alleged Infringement.

TecSec's infringement claims for the accused WebSphere products also fail because no single party—either IBM or any third party—"practice[s] each and every element of the claimed invention."[9] *BMC Res.*, 498 F.3d at 1381. As illustrated below, the method claims require that a single party perform the steps of: (i) selecting *an* object"; (ii) "encrypting *the* object"; and (iii) "decrypting *the* object."   And the system claims require a system with means for: (i) "selecting *an* object"; (ii) "encrypting *the* object"; and (iii) "accessing *the* object":

1. A method for providing multi-level multimedia security in a data network, comprising the steps of:	12. A system for providing multi-level multimedia security in a data network, comprising:
A) accessing an object-oriented key manager;	A) means for accessing an object-oriented key manager;
B) selecting an object to encrypt;	B) means for selecting an object to encrypt;
C) selecting a label for the object;	C) means for selecting a label for the object;
D) selecting an encryption algorithm;	D) means for selecting an encryption algorithm;
E) encrypting the object according to the encryption algorithm:	E) means for encrypting the object;
F) labelling the encrypted object:	F) means for labelling the encrypted object;
G) reading the object label;	G) means for reading the object label;
H) determining access authorization based on the object label; and	H) means for determining access authorization based on the label; and
I) decrypting the object if access authorization is granted.	I) means for accessing the object if access authorization is granted.

---

[8] TecSec provided no evidence of infringement under the doctrine of equivalents for this term, so TecSec's claims are limited to literal infringement. *See Schoell*, 247 F.3d at 1210.

[9] This issue applies to independent claims 1 and 12 of the '702 patent, claim 1 of the '781 patent, claim 1 of the '755 patent, and claim 1 of the '452 patent (and all claims dependent thereon).

(Ex. 3 at claims 1 and 12.) By the plain language of the claims, therefore, the method claims require that a single party *both encrypt and decrypt the same object*, and the system claims require that the system includes means for *both encrypting and accessing the same object*. *See Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1356–57 (Fed. Cir. 1999). But there is no evidence that any single party uses and/or implements an accused WebSphere product to both encrypt and decrypt the same object. Indeed, the accused products are middleware products specifically designed to facilitate communications between *two different parties*. (Chung Decl. ¶¶ 2-7; Poon Decl. ¶¶ 2-8.)

For example, the accused WebSphere Application Server product allows computer developers to create and code their own web applications running on a server that a client device can access over a network. (Chung Decl. ¶¶ 2, 5-7.)[10] Specifically, after a developer creates an application with WebSphere Application Server, a client (such as an end-user computer) may send a message (containing an "object" secured with the accused encryption functionality) over the web to the server (such as a bank server running the web application):
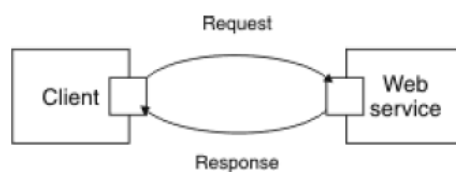
(*Id.* ¶¶ 3, 6-7.)   Under TecSec's theory of infringement, the *client* performs the claimed "selecting the object" and "encrypting the object," and the *server* hosting the web application

---

[10] Not only are at least two devices used during a web-services transaction, but the WebSphere Application Server is a programming tool that customers can use to program their own web applications however they see fit. (Chung Decl. ¶¶ 2, 5.) Thus, to work for web-services transactions such as accused by TecSec, a customer must first install, program, and configure every functionality of their implementation of WebSphere Application Server.

18

service performs the claimed "decrypting the object" or "accessing the object." (*Id.* ¶¶ 6-7.) Yet TecSec identified no evidence that the same party ever implemented both the client and server into its allegedly infringing configuration.

Similarly, in the WebSphere DataPower products, as illustrated in the diagram below, a client (such as an end-user computer) may send an encrypted "SOAP" message over the web to a server through the accused DataPower product, which decrypts the message before forwarding it to the destination server:
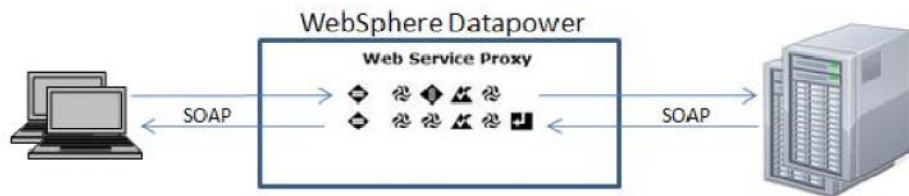
(Poon Decl. ¶¶ 6-8.) Accordingly, under TecSec's theory of infringement, the **client** performs the claimed "selecting the object" and "encrypting the object," and the accused DataPower product performs the claimed "decrypting the object" or "accessing the object." (*Id.* ¶¶ 6-8.) Yet TecSec identified no evidence that the same party ever implemented the accused DataPower products to both encrypt and decrypt the same object.

Accordingly, the accused WebSphere products do not both encrypt and decrypt the **same object**. (Chung Decl. ¶¶ 6-7; Poon Decl. ¶¶ 6-8.) TecSec's attempt to overcome this fatal flaw in its infringement case by pointing to configurations involving multiple parties fails as a matter of law, because the actions of multiple parties cannot be combined to prove infringement. *See Cross Med. Prods., Inc. v. Medtronic Sofamor Danek, Inc.*, 424 F.3d 1293, 1311 (Fed. Cir. 2005) (rejecting patentee's effort to combine the acts of surgeons with the acts of the manufacturer to find infringement); *BMC Res.*, 498 F.3d at 1381 ("[T]his court will not unilaterally restructure

the claim or the standards for joint infringement to remedy these ill-conceived claims.").

Accordingly, summary judgment in favor of IBM should be granted. *See id.* at 1380–81.

III.   The Means-Plus-Function Claims Of The '702 Patent Are Not Infringed.

Patentees are permitted to express "[a]n element in a claim for a combination ... as a

means or step for performing a specified function without the recital of structure, material, or

acts in support thereof." 35 U.S.C. § 112 ¶ 6. Indeed, a patentee's choice of the word "means"

in a claim "gives rise to 'a presumption that the inventor used the term advisedly to invoke the

statutory mandates for means-plus-function clauses.'" *Sage Prods., Inc. v. Devon Indus., Inc.*,

126 F.3d 1420, 1427 (Fed. Cir. 1997) (citations omitted). Here, the patentee drafted a number of

limitations of claims 8–9 and 12–15 of the '702 patent in means-plus-function format, as set

forth in Exhibit 1 (terms 3–19). Because, however, TecSec failed to identify any corresponding

structure for each of these means-plus-function limitations, and failed to compare the

corresponding structure to each allegedly equivalent structure in the accused systems, TecSec's

claims of infringement of these claims fail as a matter of law. *See* 35 U.S.C. § 112 ¶ 6.

A.   Claim Construction.

#	Claim Term	Proposed Construction
3–19	"means for …"	These claim elements are subject to interpretation under 35 U.S.C. § 112 ¶ 6. The recited function of each is set forth in the corresponding claims. The specification identifies no structure clearly linked to performing the recited function.

In construing each means-plus-function term, the "court must identify both the claimed

function and the corresponding structure in the written description for performing that function."

Wenger Mfg., Inc. v. Coating Mach. Sys., Inc., 239 F.3d 1225, 1233 (Fed. Cir. 2001). "In order

to qualify as corresponding, the structure must not only perform the claimed function, but the

specification must clearly associate the structure with performance of the function." *Cardiac*

Pacemakers, Inc. v. St. Jude Med., Inc., 296 F.3d 1106, 1113 (Fed. Cir. 2002). "This duty to link or associate structure to function is the *quid pro quo* for the convenience of employing § 112, ¶ 6." *B. Braun Med., Inc. v. Abbott Labs.*, 124 F.3d 1419, 1424 (Fed. Cir. 1997).

The claimed function of each means-plus-function limitation is explicitly recited in the claim (*e.g.*, "limiting object access," "embedding a first object within a second object," etc.), as set forth in Exhibit 1. *See Micro Chem., Inc. v. Great Plains Chem. Co.*, 194 F.3d 1250, 1258 (Fed. Cir. 1999). The '702 patent fails, however, to identify any corresponding structure for performing each of these functions. (Ex. 3.) For example, there is no disclosed structure for performing the function of "limiting object access," "embedding a first object within a second object," or any of the other claimed functions. (*Id.*) And there is nothing in the specification that "clearly links" any structure to each of these claimed functions. *See Default Proof Credit Card Sys., Inc. v. Home Depot U.S.A., Inc.*, 412 F.3d 1291, 1298 (Fed. Cir. 2005) ("A structure disclosed in the specification qualifies as 'corresponding' structure *only* if the specification or prosecution history clearly links or associates that structure to the function recited in the claim.").

Evidencing the fact that the '702 patent specification fails to identify any corresponding structure for performing each of the claimed functions, TecSec was unable to identify any support in the patent for these elements during discovery. For example, IBM's Interrogatory No. 19 specifically asked TecSec to identify the support for each asserted claim limitation:

> **INTERROGATORY NO. 19:**
>
> Separately, for each element of each asserted claim of each Patent-in-Suit, identify all support for that claim element in the specification by reference to the specific column and line numbers and/or applicable portions of the figures of the issued patent and by reference to the specific page and line numbers and/or applicable portions of the figures of the earliest-filed application to which the patent claims priority.

(Ex. 11 at 2.) But TecSec identified no support whatsoever. (*Id.* at 2–3.) Accordingly, the Court should construe each term as lacking corresponding structure, as set forth in Exhibit 1.

B.   IBM Does Not Infringe The Means-Plus-Function Claims.

To prove infringement of any claim including a means-plus-function limitation, including

claims 8–9 and 12–15 of the '702 patent, TecSec must show that the accused device performs the

recited function with structure that is the same as or equivalent to the corresponding structure in

the patent specification. *See* 35 U.S.C. § 112 ¶ 6; *Baran v. Med. Device Techs., Inc.*, 616 F.3d

1309, 1316–17 (Fed. Cir. 2010). But neither TecSec nor its expert performed this analysis. This

failure to identify the structure in the specification for each means-plus-function limitation, and

to compare this structure to the accused structure of each accused product, is fatal to TecSec's

infringement claims, and precludes a finding of infringement as a matter of law:

> Infringement of a means-plus-function limitation "requires that the
> relevant structure in the accused device ... be identical or
> equivalent to the corresponding structure in the specification." ***To
> establish infringement under § 112, ¶ 6, it is insufficient for the
> patent holder to present testimony "based only on a functional,
> not a structural, analysis." Here, [Plaintiff] failed to identify the
> structure in the specification that is the "temperature controller
> means" and compare it to the structure of the accused device.
> Accordingly,*** because [Plaintiff] failed to present substantial
> evidence of infringement of claim 13 of the '693 patent, ***the jury
> verdict of infringement of claim 13 must be reversed***.

CytoLogix Corp. v. Ventana Med. Sys., Inc., 424 F.3d 1168, 1178 (Fed. Cir. 2005) (citations

omitted); *see also Alpex Computer Corp. v. Nintendo Co.*, 102 F.3d 1214, 1222 (Fed. Cir. 1996)

(reversing verdict of infringement because plaintiff's expert "did not compare the structure of the

[accused product] with the bit map structure disclosed in the specification.").   Summary

judgment of no infringement of these claims should thus be granted. *See Novartis Corp. v. Ben*

Venue Labs., Inc., 271 F.3d 1043, 1054 (Fed. Cir. 2001).

IV.   IBM's WebSphere Products Do Not Infringe The '433 Patent.

TecSec also accuses the same IBM WebSphere products identified above in section II of

infringing the asserted claims of the '433 patent. As set forth below, TecSec's infringement

claims fail as a matter of law because: (i) none of the accused WebSphere products "provide" an object or a first computer readable medium; and (ii) the accused Websphere Application Server, DataPower XML Security Gateway XS40, and DataPower Integration Appliance XI50 products do not "store" encrypted data.

A.   The Accused WebSphere Products Do Not "Provide" An Object Or A First Computer Readable Medium Having Stored Thereon A First Data Set.

Every independent claim of the '433 patent requires "*providing* … at least one object relating to a process" or "*providing* a first computer readable medium having stored thereon a first data set." (Ex. 12 at claims 1–7, 10.)   There is no genuine dispute, however, that the accused WebSphere products do not perform these steps. Indeed, any data or object that is encrypted by the accused WebSphere products must be *received* by the products from an external source—the products themselves simply do not "provide" such data.[11] (Chung Decl.¶ 10; Poon Decl.¶ 11.)

Moreover, TecSec identifies no evidence that the accused products "provide" anything.[12] Instead, TecSec contends this limitation is met simply because the accused products can *receive* and encrypt XML documents.   But TecSec cannot rewrite the plain term "providing" as "receiving," so that it can cobble together an infringement theory. *See Chef Am., Inc. v. Lamb-Weston, Inc.*, 358 F.3d 1371, 1374 (Fed. Cir. 2004) ("Thus, in accord with our settled practice we construe the claim as written, not as the patentees wish they had written it.").   Indeed, under

---

[11] Similarly, there is no evidence that IBM or any other party ever provides "a first computer readable medium having stored thereon a first data set." Indeed, no such data set exists in the products as sold, and IBM does not otherwise provide a "computer readable medium" with such data. (Chung Decl. ¶ 10; Poon Decl. ¶ 11.)

[12] TecSec provided no evidence of infringement under the doctrine of equivalents for this term, so TecSec's claims are limited to literal infringement. *See Schoell*, 247 F.3d at 1210.

TecSec's interpretation, the "providing" step has no meaning, which is improper. *See Cat Tech LLC v. TubeMaster, Inc.*, 528 F.3d 871, 885 (Fed. Cir. 2008) ("[C]laims are interpreted with an eye toward giving effect to all terms in the claim." (citation omitted)). Accordingly, because there is no genuine dispute that the accused WebSphere products do not perform the "providing" steps, summary judgment of no infringement should be granted. *See Anderson*, 477 U.S. at 249.

B.   The Accused WebSphere Products Do Not "Store" Encrypted Information.

1.   Claim Construction.

#	Claim Term	Proposed Construction
20	"storing"	"transferring information to (or retaining information in) a device from which it can be obtained at a later time"

The patent specification repeatedly and consistently explains that the objects of the invention may be handled in one of two ways after they are encrypted—they may be *either* passed directly to authorized recipients *or* stored and forwarded at a later time:

(Ex. 12 at 5:46–49, 5:67–6:3; *see also id*. at 6:20–24, 6:56–60.)

The plain language of the claims covers only the "storing" alternative. (*Id.* at 7:4–5 ("*storing* the encrypted at least a portion of the first object *for subsequent use* by an intended recipient.").)   The alternative—passing the information on a real-time basis to intended recipients—is thus dedicated to the public and, as a matter of law, the claims cannot be rewritten to cover this alternative. *See Unique Concepts, Inc. v. Brown*, 939 F.2d 1558, 1562–63 (Fed. Cir. 1991) ("It is also well-established that subject matter disclosed but not claimed in a patent

application is dedicated to the public."); *PSC Computer Prods., Inc. v. Foxconn Int'l, Inc.*, 355

F.3d 1353, 1360 (Fed. Cir. 2004) ("The disclosure-dedication rule requires an inventor who

discloses specific matter to claim it, and to submit the broader claim for examination. Otherwise,

that matter is dedicated to the public….").

The use of the term "storing" in the patent claims and specification is consistent with the

ordinary and customary meaning of the term—"transferring information to (or retaining

information in) a device from which it can be obtained at a later time":

> **store:** 1. To transfer an element of information to a device from which the unaltered information can be obtained at a later time. 2. To retain data in a device from which it can be obtained at a later time. 3. The British term for storage.

(Ex. 13 at 478; *see also* Ex. 14 at 1201.) Indeed, claims 1–6 expressly require "storing … *for*

subsequent use" (Ex. 12), and claims 7 and 10 expressly require "storing" on a "computer

readable medium" (*id.*). The context in which the term "storing" is used in the claims thus

supports adoption of the ordinary and customary meaning, *i.e.*, "transferring information to (or

retaining information in) a device from which it can be obtained at a later time." *See Phillips*,

415 F.3d at 1314 ("To begin with, the context in which a term is used in the asserted claim can

be highly instructive."). And as set forth above, the specification uses the term the same way.

Accordingly, "storing" should be construed as set forth above. *See id.* at 1312.

> ### 2.   There Is No Dispute That The Accused WebSphere Products Do Not "Store" Encrypted Information During the Accused Functionality.

Every independent claim of the '433 patent requires "storing" the encrypted information

(or the second data set, which is encrypted), which as set forth above, requires "transferring

information to (or retaining information in) a device from which it can be obtained at a later

time." (Ex. 12 at claims 1–7, 10.) But the WebSphere products[13] have no capability of "storing"

encrypted messages. Rather, they are designed to pass encrypted messages directly on a real-

time basis to recipients for immediate decryption. (Chung Decl. ¶ 11; Poon Decl. ¶¶ 14-15.)

Indeed, these products are designed to receive messages from external sources, process the

messages as fast as possible, and then immediately send the messages to the intended recipients.

(Chung Decl. ¶¶ 2, 11; Poon Decl. ¶¶ 2, 14-15.)   But this is precisely what the '433 patent

distinguished from "storing" and did not claim. (Ex. 12 at 5:45–49 ("The encrypted objects are

then ***either passed directly on a real-time basis*** to authorized recipients for immediate

decryption and further processing, ***or they are stored*** and forwarded at a later time."); 6:1–3.)

TecSec's expert tries to overcome this deficiency by pointing to "system memory" which

maintains information as it is processed by the products. (Ex. 17 at 160.)[14] But this is clearly not

the claimed "storing," as the products process the information as quickly as possible and, as they

finish, pass it "directly on a real-time basis to authorized recipients for immediate decryption."

(Chung Decl. ¶¶ 2, 11; Poon Decl.¶¶ 2, 14-15.)   Accordingly, because TecSec's allegations

attempt to encompass what it disclosed but did not claim, its infringement claim fails as a matter

of law.[15] *See Schoenhaus v. Genesco, Inc.*, 440 F.3d 1354, 1359 (Fed. Cir. 2006) (finding a

disclosed but not claimed feature "dedicated to the public" and therefore "the district court

properly granted summary judgment of non-infringement"); *Maxwell v. J. Baker, Inc.*, 86 F.3d

---

[13] IBM is not moving on this limitation for the DataPower XB60 product.

[14]   TecSec's expert also identifies a feature called a "Message Store" for the WebSphere Application Server product. But this feature is entirely irrelevant because it stores ***unencrypted*** messages, not encrypted messages as required by the claim. (Chung Decl. ¶¶ 12-13.)

[15] TecSec provided no evidence of infringement under the doctrine of equivalents for this term, so TecSec's claims are limited to literal infringement. *See Schoell*, 247 F.3d at 1210.

1098, 1107 (Fed. Cir. 1996) ("We have frequently applied this rule to prohibit a finding of literal infringement when an accused infringer practices disclosed but unclaimed subject matter.").

V.   IBM's System Z Products Do Not Infringe The '448 Patent.[16]

TecSec accuses the following IBM System z products of infringing the '448 patent:

- System z mainframe servers (z9 and z10) that incorporate Crypto Express2; and
- System z mainframe servers (z9 and z10) that incorporate Crypto Express3.

But TecSec's infringement claims fail because these products do not include a "format filter adapted to extract control data and main data from the input data." (*See* Ex. 15 at 6:29–30.) Specifically, TecSec alleges that "ICSF"—the interface program between a System z mainframe and a Crypto Express feature—meets this limitation. But there is no genuine dispute that ICSF does not "*extract*" anything, nor does TecSec identify any evidence that it does. Rather, upon receipt of a processing request, ICSF *combines* the data to be processed ("main data") *together with other data*, such as the request-type ID and cryptographic keys ("control data"), into a *single data structure* to be sent to the Crypto Express. (Arnold Decl. ¶¶ 6–11.)

Moreover, this difference is not "insubstantial." As the Court recognized, separation of "control data" and "main data" by a "format filter" is crucial to the invention. (D.I. 459 at 37.) Thus, because ICSF performs *the opposite* of extracting—by *combining* "control data" and "main data"—it cannot meet the "format filter" limitation literally or by equivalents. Summary judgment of no infringement should be granted. *Planet Bingo, LLC v. GameTech Int'l, Inc.*, 472 F.3d 1338, 1345 (Fed. Cir. 2006) ("This court has refused to apply the doctrine [of equivalents] in … cases where the accused device contained the antithesis of the claimed structure.").

---

[16] A description of the accused IBM System z products is provided in the declaration of Todd Arnold, filed concurrently herewith.

VI.   TecSec's Indirect Infringement Claims Fail As A Matter Of Law.

      A.   There Is No Evidence Of Direct Infringement By Any Third Party.

As a prerequisite to proving that IBM indirectly infringed any claim, TecSec must first show that some third party committed the entire act of direct infringement of such claim. *See BMC Res.*, 498 F.3d at 1379. But TecSec failed to identify any evidence of direct infringement by any third party for any of the asserted patent claims. Significantly, IBM expressly asked TecSec to provide "an identification of each person that TecSec contends directly infringed" each asserted patent claim in support of its inducing infringement and contributory infringement claims. (Ex. 11 at 13–14.) TecSec provided no response. (*Id.* at 13–15.) Nor has TecSec's expert identified any such direct infringer. This inability to identify any actual instances of alleged direct infringement is striking given that TecSec *served over 55 subpoenas on IBM's customers*, trying in vain to uncover an instance of its hypothetical direct infringement. (Deoras Decl. ¶ 28.) Yet despite this massive effort, TecSec failed to identify *even one* alleged instance of direct infringement. TecSec's indirect infringement claims thus fail as a matter of law. *See DSU Med.*, 471 F.3d at 1303 ("[T]he patentee always has the burden to show direct infringement for each instance of indirect infringement."); *Fujitsu Ltd. v. Netgear Inc.*, 620 F.3d 1321, 1329 (Fed. Cir. 2010) ("Unless the claim language only requires the capacity to perform a particular claim element, we have held that it is not enough to simply show that a product is capable of infringement; the patent owner must show evidence of specific instances of direct infringement."); *ACCO Brands*, 501 F.3d at 1313 ("In order to prove direct infringement, a patentee must either point to specific instances of direct infringement or show that the accused device necessarily infringes the patent in suit.").

      B.   There Is No Evidence Of Inducing Infringement By IBM.

Even if TecSec could show that some third-party directly infringed any of the asserted

claims, TecSec failed to identify any evidence that IBM induced the alleged infringement. Indeed, in response to IBM's interrogatory seeking TecSec's bases for its claims that IBM induced infringement under 35 U.S.C. § 271(b), TecSec identified nothing to support a finding that IBM specifically intended to cause the alleged infringement. (Ex. 11 at 13–14.) Instead, TecSec merely referenced its infringement contentions and expert reports, but neither contain *any* evidence that IBM intended to cause infringement. Accordingly, summary judgment of no inducement should be granted. *See Vita-Mix Corp. v. Basic Holding, Inc.*, 581 F.3d 1317, 1329 (Fed. Cir. 2009) (affirming grant of summary judgment of no inducement based on lack of evidence that the defendant intended to encourage infringement); *Warner-Lambert*, 316 F.3d at 1365 (affirming summary judgment of no inducement because "[e]specially where a product has substantial noninfringing uses, intent to induce infringement cannot be inferred even when the defendant has actual knowledge that some users of its product may be infringing the patent.").

C.   There Is No Evidence Of Contributory Infringement By IBM.

There is also no evidence that IBM contributed to the infringement of any third party. Indeed, in response to IBM's interrogatory seeking TecSec's bases for its claims that IBM contributed to infringement under 35 U.S.C. § 271(c), TecSec again merely referenced its infringement contentions and expert reports, which are completely devoid of any supporting evidence. (Ex. 11 at 14–15.) Moreover, there is no genuine dispute that the accused products can be used in many different ways that do not infringe the patents-in-suit, even under TecSec's theories—and TecSec proffered no evidence to the contrary. Nor did TecSec come forward with evidence that IBM had the requisite knowledge required by 35 U.S.C. § 271(c). But TecSec must show that IBM "knew that the combination for which its components were especially made was both patented and infringing." *Golden Blount, Inc. v. Robert H. Peterson Co.*, 365 F.3d

29

1054, 1061 (Fed. Cir. 2004). Because TecSec identified no such evidence, summary judgment

of no contributory infringement should be granted. *See Anderson*, 477 U.S. at 249.

VII.   Additional Claim Terms.

Several additional claim terms should be construed as set forth in Exhibit 1 as follows:

#	Claim Term	Proposed Construction
21	"selecting" ('702 patent)	"choosing from among several"
22	"a parallel processor array that includes a plurality of processors" ('448 patent)	"two or more processors each adapted to concurrently process a portion of main data according to a particular cryptographic function"
23	"extract control data and main data from the input data" ('448 patent)	"separate out the control data and main data from the input data"
24	"distribute" ('448 patent)	"to divide and dispense in portions"

To the extent TecSec disputes any of these constructions, IBM is prepared to submit additional

briefing, if requested. *See O2 Micro Int'l Ltd. v. Beyond Innovation Tech. Co.*, 521 F.3d 1351,

1362 (Fed. Cir. 2008) ("When the parties present a fundamental dispute regarding the scope of a

claim term, it is the court's duty to resolve it."). And to the extent that TecSec offers a

construction for any other terms, IBM reserves its right to offer a competing construction.

<u>CONCLUSION</u>

For the foregoing reasons, IBM respectfully requests that this Court construe the claims

as set forth above and grant its Motion for Summary Judgment of No Infringement.

Dated: January 21, 2011   Respectfully submitted,

                /s/ Craig C. Reilly
             Craig C. Reilly, Esq. (VSB # 20942)
             111 Oronoco Street
             Alexandria, Virginia 22314
             Telephone: 703-549-5354
             Facsimile: 703-549-2604
             E-mail: craig.reilly@ccreillylaw.com
             Counsel for Defendant IBM

Of Counsel for Defendant IBM:

John M. Desmarais
DESMARAIS LLP
230 Park Avenue
New York, NY 10169
Telephone: 917-340-6940
Facsimile: 914-666-6962

Jon T. Hohenthaner
KIRKLAND & ELLIS LLP
601 Lexington Avenue
New York, NY 10022-4675
Telephone: 212-446-4800
Facsimile: 212-446-4900

Elizabeth Bernard
KIRKLAND & ELLIS LLP
655 15th Street, N.W.
Washington, D.C. 20005
Telephone: 202-879-5000
Facsimile: 202-879-5200

CERTIFICATE OF SERVICE

I hereby certify that on this 21st day of January 2011, a true and correct copy of the foregoing pleading or paper was served using the Court's CM/ECF system, with electronic notification of such filing to the following counsel of record:

Brian M. Buroker
HUNTON & WILLIAMS
1900 K Street NW
Washington, DC 20006-1109
Telephone: 202-955-1500
Facsimile: 202-778-2201
E-mail: bburoker@hunton.com
Counsel for Plaintiff

                                        /s/ Craig C. Reilly
                                Craig C. Reilly, Esq. (VSB # 20942)
                                111 Oronoco Street
                                Alexandria, Virginia 22314
                                Telephone: 703-549-5354
                                Facsimile: 703-549-2604
                                E-mail: craig.reilly@ccreillylaw.com
                                Counsel for Defendant IBM